❒ Original ❒ I

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
information associated with the accounts stored at Microsoft Corporation, (Subject Accounts 1 and 2) cbailey@lsq.com and rlee@lsq.com (See Attachments)

Case No. 23-M-348 (SCD)
Matter No.: 2021R00461

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____
(identify the person or describe the property to be searched and give its location):

See Attachment A, over which this Court has jurisdiction pursuant to 18 U.S.C. §§ 2703 and 2711 and Federal Rule of Criminal Procedure 41.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 4-4-23 *(not to exceed 14 days)*

❒ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Stephen C. Dries.
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____.

Date and time issued: 3-22-23. 2:45 pm

Stephen C. Dries
Judge's signature

City and state: Milwaukee, Wisconsin

Hon. Stephen C. Dries, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Grand Jury Matter Number 2021R00461

PROPERTY TO BE SEARCHED

This warrant applies to information associated with the following accounts that are stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, a company headquartered at One Microsoft Way, Redmond, WA 98052 (Subject Accounts 1 and 2):

1. cbailey@lsq.com
2. rlee@lsq.com

ATTACHMENT B

Grand Jury Matter Number 2021R00461

PARTICULAR THINGS TO BE SEIZED

I. Information to be disclosed by Microsoft Corporation (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to the request made under 18 U.S.C. § 2703(f) on January 4, 2023, the Provider is required to disclose the following information to the government for the accounts or identifiers listed in Attachment A:

a. The contents of all emails associated with the accounts from January 1, 2019 until the date of this warrant, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the

account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and

f. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within 21 days of the issuance of the warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18, United States Code, Sections 371 and 1343 involving Cherie Campion, Engstrom Inc., LSQ Funding Group, L.C., Carrie Bailey, and Richard Lee, those violations occurring after January 1, 2019, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Evidence of fraud, conspiracy, and related activity in connection with the purchase, sale, and payoff of invoices;

b. Evidence indicating knowledge and concealment of false invoices;

c. Evidence of financial transactions related to the purchase, sale, and payoff of invoices;

d. Evidence of audits, examinations, and background checks;

e. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

f. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

g. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

h. The identity of person(s) who communicated with the account about matters relating to the criminal violations described above, including records that help reveal their whereabouts.

UNITED STATES DISTRICT COURT

for the

_____ District of _____

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

information associated with the accounts stored at Microsoft Corporation, (Subject Accounts 1 and 2) cbailey@lsq.com and rlee@lsq.com (See Attachments)

Case No. 23-M-348 (SCD)

Matter No.: 2021R00461

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 371 and 1343	Conspiracy and Wire Fraud.

The application is based on these facts:

☑ Continued on the attached sheet.

☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SA Sean Sweeney, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone *(specify reliable electronic means)*.

Date: 3-22-23

Judge's signature

City and state: Milwaukee, Wi

Hon. Stephen C. Dries, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

Grand Jury Matter Number 2021R00461

I, Sean Sweeney, being duly sworn, state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation (FBI). I have been so employed for approximately 7 years.

2. As part of my duties as a Special Agent, I am assigned to the FBI Milwaukee Field Office. I am currently focused on the investigation of financial crimes, including wire fraud, in violation of Title 18, United States Code, Section 1343; mail fraud, in violation of Title 18, United States Code, Section 1341; bank fraud, in violation of Title 18, United States Code, 1344; and other financial crimes. I have participated in the execution of multiple federal search warrants.

3. I make this affidavit in support of the application for a search warrant for information associated with certain accounts that are stored at premises controlled by Microsoft Corporation ("Microsoft"), an email and electronic services provider headquartered at One Microsoft Way, Redmond, WA 98052. The accounts to be searched are cbailey@lsq.com ("Subject Account 1") and rlee@lsq.com ("Subject Account 2"), which are further described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant pursuant to Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Microsoft to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of

Attachments B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

4. As set forth below, there is probable cause to believe that in Subject Account 1 and Subject Account 2 contain the fruits, evidence, and instrumentalities of criminal offenses in violation of Title 18, United States Code, Section 371 (conspiracy) and Section 1343 (wire fraud) (the Subject Offenses).

5. The statements in this affidavit are based on my personal knowledge, subpoenaed records and documents obtained during the investigation, information I have received from other law enforcement personnel and from persons with knowledge regarding relevant facts. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are sufficient to establish probable cause to believe that evidence and instrumentalities of the Subject Offenses are located in Subject Account 1 and Subject Account 2.

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined in 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated, see 18 U.S.C. § 2711(3)(A)(i).

FACTS SUPPORTING PROBABLE CAUSE

Overview

7. "Factoring" is, broadly speaking, a financial transaction in which a business sells its accounts receivable to a third party at a discount. Federal law enforcement is investigating allegations that Cherie Campion (Campion), the owner/CEO of Engstrom, Inc. (Engstrom), defrauded her longtime factoring company, LSQ Funding Group, L.C. (LSQ). LSQ purchased Engstrom's invoices and was repaid when it collected payment on the invoices. However, over the course of years, Campion submitted millions of dollars of false invoices to LSQ. When LSQ discovered the fraud, Campion found a second factoring company, Millennium Funding (Millennium), who unknowingly purchased over $10 million in fraudulent invoices from LSQ in January 2020. Millennium discovered Campion's fraud scheme within a few weeks of purchasing the fraudulent invoices. On April 15, 2020, Campion filed Chapter 11 Bankruptcy in the Eastern District of Wisconsin for Engstrom.

8. Federal law enforcement is also investigating related allegations that LSQ, after it discovered it had been defrauded by Campion, knowingly sold millions of dollars of worthless invoices to Millennium. Carrie Bailey (Bailey), an LSQ Portfolio Manager, had primary responsibility for LSQ's factoring relationship with Engstrom until January 29, 2020, when LSQ's relationship with Engstrom was terminated. As explained below, there is a specific and articulable basis to believe that evidence related to LSQ's discovery that the invoices were worthless and LSQ's

intentional sale of worthless invoices to Millennium, is contained within the Subject Accounts 1 & 2.

Scheme

9. Engstrom was incorporated in January 1993 and operated out of Manitowoc, Wisconsin. Engstrom purported to provide temporary staffing to various businesses, specifically utility and energy companies. Campion relied on accounts receivable factoring to fund Engstrom's business. Factoring provides a client (Engstrom) with a line of credit based on funds it expects to receive from its customers. In a typical factoring relationship, a client submits invoices to its customers and to the factor. After purchasing the invoice, the factor advances a certain percentage of the invoice's face value to the client as an initial payment. Once the client's customers submit payment upon the invoice directly to the factor (LSQ), the factor remits the outstanding value of the invoice, less fees and interest, to the client (Engstrom).

10. The funding structure relies on the creditworthiness of the client's customers instead of the client. Thus, factors must ensure that those customers are both able to pay the outstanding invoices and that such invoices are legitimate, accurate, and owing. Factors generally take great care to ensure that payments are remitted directly to the factor (LSQ) and not to the client (Engstrom).

11. Based on witness interviews, court filings, Wisconsin Secretary of State records, bank records, and business records obtained pursuant to grand jury subpoenas, Engstrom's factoring relationship with LSQ began in December 2014 and

ended in January 2020. During their relationship, Engstrom submitted over $200 million of invoices to LSQ, which LSQ purchased. The vast majority of those invoices purported to be issued to Engstrom's customer, NextEra Energy (NextEra), a Florida-based energy company with a facility in northeastern Wisconsin. However, records obtained from NextEra show that only about $1.5 million of legitimate invoices were submitted by Engstrom while LSQ was their factor. Therefore, records show that the majority of invoices Campion submitted to LSQ were false.

12. Campion was able to conceal the scheme for years by increasing the value of the invoices over time to cover LSQ's fees and to fund a lavish lifestyle for herself and her family. As described below, Campion concealed her scheme further by creating a shell company using NextEra's likeness and opening bank accounts using NextEra's likeness. Campion used these accounts to funnel the majority of LSQ's money back to LSQ, leading LSQ to believe that NextEra was paying them directly.

13. Records subpoenaed from Bank First show that business checking account ending 2288 (Account 2288) in the name of Engstrom Inc was opened in 2006. Campion, her husband Steven Campion, and her son Joshua Campion are signors on the account. For the period 2016 to 2020, LSQ wire transferred a total of approximately $199,111,960 to Account 2288. Campion primarily used the funds Engstrom received from LSQ to live a lavish lifestyle and to pay back LSQ. The following are examples of Campion's use of funds in Account 2288:

- Approximately $36,841,238 was wire transferred back to LSQ.

- Approximately $156,984,272 was wire transferred to Engstrom, Inc. DBA NextEra Renewable Energy account ending 6522 at Bank of America.

- Approximately $1,170,281 was paid as salaries and bonuses to Campion, her husband Steve, her son Joshua, and her daughter-in-law Angela.

- On December 13, 2016, Campion issued check number 9302 for $9,115.04 to Lakewood Motorsports. Records obtained from Lakewood Motors show that this check was for the purchase of a snowmobile.

- On October 17, 2018, $29,700 was wire transferred to an individual with initials J.M. Records obtained from J.M. show that the wire was for the purchase of a buckskin horse.

14. Records subpoenaed from Bank of America show that on September 8, 2014, Campion opened business checking account ending 6522 in the name of Engstrom, Inc. DBA NextEra Renewable Energy (Account 6522). Campion is the sole signor on Account 6522. From 2016 to 2020, Account 6522 was primarily funded by wire transfers from Account 2288, totaling approximately $156,984,272. The following are examples of Campion's use of funds in Account 6522:

- Approximately $75,198,161 was transferred intrabank to LSQ.

- Approximately $81,555,178 was transferred intrabank to NextEra Renewable ES LLC account ending 7135.

- On September 12, 2017, $30,000 was wire transferred to an individual with initials A.T., referencing "PERSONAL HORSE PURCHASE CEO". Records obtained from A.T. show that the wire was for the purchase of a horse.

- On September 26, 2019, $29,759.15 was wire transferred to Love County Closing. Records obtained from Love County Closing, LLC show that this wire was the initial deposit for Campion's purchase of real property in Wilson, OK.

15. Records subpoenaed from Bank of America show that on February 11, 2015, Campion opened business checking account ending 7135 in the name of NextEra Renewable ES LLC (NextEra ES) (Account 7135). This was eight days after Campion registered NextEra ES with the State of Wisconsin. Campion is the sole signor on Account 7135. From 2016 to 2020, Account 7135 was solely funded by transfers from Account 6522 totaling approximately $81,555,178. These funds were used to transfer a total of approximately $80,419,978 to LSQ.

16. Records, including emails between LSQ employees, indicate LSQ realized some of the payments—which were supposed to be remitted by NextEra—were in fact remitted by Engstrom. As detailed below, LSQ employee emails obtained from court filings in Engstrom's Bankruptcy case show their concerns regarding payments coming directly from Engstrom.

17. On February 21, 2017, LSQ Staff Accountant Gina Enciso emailed Linda Nissen, Rodney Campos, Luz Hernandez, and Richard Lee[1]. The email subject line stated, "Audit Cash Application Test Selection – Engstrom". In the body of the email, Enciso stated in part, "The below item was selected by the BOA auditor. Please note that both the remittance and payment were sent by the client; please advise when we stopped receiving payment directly from the customer." LSQ Account Manager Linda

[1] This email is in pdf format and does not show the email address for Richard Lee, but it lists his name as a recipient.

Nissen (Nissen) responded to this email and only sent it to Rodney Campos. In her response, Nissen stated in part, "Whenever Nextera does an update to their system, the payments would default to the original bank (client bank). The client would then forward any payments to our bank. She would then go into the Nextera system and correct the banking. Supposedly as of the end of the year, Nextera put in an upgrade to avoid payments defaulting back to the original bank. There have been few to none since."

18. On May 18, 2017, LSQ received a wire confirmation email showing Engstrom sent LSQ $132,631.88. This email was forwarded to LSQ's Assistant VP Account Executive Sara Flegel (Flegel) and Nissen. Flegel responded to this email and only sent it to Nissen. In her response, Flegel stated in part, "This is a problem. On 100% concentration at this NFE level, it needs to be clear that remittance can't be changed. It should be clear to the customer as well."

19. On July 5, 2017, LSQ received a wire confirmation email showing Engstrom sent LSQ $471,986.40. This email was forwarded to Flegel and Nissen. Flegel responded to this email and only sent it to Nissen. In her response, Flegel stated, "This is a very large payment to be going to the client. We need to figure out a way to confirm direct with the customer that the NOA has been acknowledged. We need to be able to reach out to the customer direct, please ask the client how we can accomplish this and see if she has any ideas."

20. On October 23, 2018, LSQ received a wire confirmation email showing Engstrom sent LSQ $110,986.00. This email was forwarded by Diane Mills to Bailey

at Subject Account 1. Bailey responded to Mills' email stating, "Pardon me if this is too big of an ask, but is there a way to pull the full payment report that has come directly from the client within the last year?" Mills responded to Bailey's email stating in part, "A quick way to get a rough estimate of the number of payments (mostly wires) that list Engstrom as Originator is by doing a search for Engstrom as Payor in FS, I put in 1/1/18 as start date & got 230 hits."

21. Despite such concerns, LSQ continued to purchase invoices and issue payments to Engstrom until early January 2020. As described below, it is alleged that LSQ eventually discovered the scheme, subsequently terminated its factoring relationship with Engstrom on January 9, 2020, and demanded Engstrom repurchase any invoice that remained unpaid. When LSQ terminated its factoring relationship with Engstrom, there were over $10 million of outstanding fraudulent invoices LSQ had purchased and was owed. Campion subsequently arranged for an unwitting second factor, Millennium, to purchase the fraudulent invoices she sold to LSQ.

22. On December 13, 2019, May Garcia, LSQ's Verification Manager, emailed Richard Lee (Lee), LSQ's Chief Risk Officer, at Subject Account 2. In the email, Garcia made the following statements:

- "Engstrom is a DO NOT CONTACT client. I have always said this proves to be rather difficult for LSQ to independently confirm legitimate invoices at any given point."
- "Such a large scale business out of her home?"
- "A lot of communication coming directly from client. Red flag."

- "Verification Team needs go ahead to independently confirm all open invoices."

23. On December 13, 2019, Lee responded to Garcia's email using Subject Account 2. Lee emailed Garcia, Bailey at Subject Account 1, and Tony Gianfransico. In the email, Lee stated in part, "Next steps are with Carrie to try to verify open invoices with Nextera. We do receive fax confirmation from debtor. Of course, there is risk that it could be fraudulent, but that is what we are trying to verify."

24. Unbeknownst to Campion, Bailey inquired with NextEra about Engstrom's account after receiving direction from Lee. Using Subject Account 1, Bailey sent an email to NextEra's accounts payable department on December 13, 2019. Bailey asked NextEra to provide an open balance statement for Engstrom. On December 16, 2019, a NextEra contractor working in the procurement department informed Bailey, in an email to Subject Account 1, that NextEra did not have any open invoices for Engstrom. Bailey, using Subject Account 1, quickly asked NextEra to confirm the last payment it processed for Engstrom. The next day, December 17, 2019, the NextEra contractor, in an email to Bailey's Subject Account 1, informed Bailey the last payment NextEra issued to Engstrom was paid on June 20, 2019 and totaled approximately $340[2]. Later that evening, Bailey, again using Subject Account 1, forwarded the NextEra contractor's email to Lee at Subject Account 2. At that point, Bailey had seemingly identified a significant discrepancy because LSQ factored

[2] This payment information was corroborated through records received from NextEra pursuant to a subpoena.

tens of millions of dollars of NextEra invoices for Engstrom between June and December 2019.

25. On or about January 6, 2020, Campion spoke to Bailey and Lee by telephone. The details of their telephone conversation are seemingly outlined in a letter provided to the Government by Campion's criminal defense attorney. The letter, dated September 27, 2022, advises Bailey and Lee called Campion because LSQ was unable to verify (1) Engstrom's invoices and (2) that Engstrom was truly a supplier of NextEra. During the call, the letter indicates, Bailey and Lee also voiced concerns that Engstrom was paying previous invoices with newly factored money.

26. In his letter, Campion's attorney included several apparent quotations, captured during conversations with his client (Campion), about the January 6, 2020 telephone call:

> *"Rich stated that it seems as if I am paying them back on invoices from the schedules funded."*
>
> *"He asked if Engstrom was a legitimate business. I stated that, yes, it was. He stated that it is a felony and fraud to produce invalid invoices and everyone could be charged with this."*
>
> *"He stated during phone call and once more at the end I need to be very transparent with them and if I work with them, they would work with me. At the end of the phone call . . . I stated that I needed to soak everything in and would make sure that Chris contacted Carrie (Bailey) as requested."*
>
> *"I also stated that it seemed to me that they wanted me to find alternative financing and he stated that they would be obliged with that."*
>
> *"At end of call when he stated about being transparent again, he said that I had until morning to think about everything and get back with them."*

27. On or about January 9, 2020, the letter continues, Campion spoke to Bailey again by telephone. This time, Bailey was accompanied on the telephone by

LSQ's CEO, Dan Ambrico (Ambrico). The details of this additional telephone call were also outlined in the letter provided by Campion's attorney.

28. During the call, Campion's attorney writes, Ambrico reiterated concerns that Engstrom was paying old invoices with funds acquired from newly factored invoices. Ambrico and Bailey accused Campion of fraud and demanded she repay LSQ within two weeks.

29. Campion's attorney again included several quotations, captured during conversations with his client, about the January 9, 2020 telephone call:

> *Ambrico talked about "the consequences of invalid invoices and felony and fraud. He stated a few times that I needed to be very transparent with them and they would work with me if I would work with them."*
>
> *"He also stated it sure looks as if I am paying back invoices from the money I receive from them."*
>
> *"I finally at end just stated to Dan in the last phone call that I would try and get them paid back with another source within two weeks. He said are you sure, I said yes, I am sure."*
>
> *"He stated that maybe we should meet and talk face to face about all this and I stated that I didn't see a need to. He stated that he probably should have done this before hand since it was 5 years since Brian Keuper3 visited."*
>
> *"Dan stated to keep them updated with progress regularly on paying them off within the 2 week period."*

30. Campion believes the telephone calls occurring on or about January 6, 2020 and January 9, 2020 originated from Bailey's personal cell phone. Telephone records obtained via grand jury subpoena revealed Campion received a telephone call from (727) 455-7572 on January 6, 2020 at approximately 12:04 p.m., which lasted 21 minutes. The same telephone records revealed Campion placed a telephone call to (727) 455-7572 on January 9, 2020 at approximately 11:34 a.m., which lasted 11

minutes. A query of law enforcement databases revealed telephone number (727) 455-7572 is associated with Bailey.

31. The existence of the telephone calls has been discussed in ongoing litigation between Millennium and LSQ in Florida. In a December 5, 2022 filing, LSQ admitted Lee spoke with Campion on or about January 6, 2020. LSQ also admitted Bailey and Ambrico spoke with Campion on or about January 9, 2020. It should be noted, however, that LSQ has denied (1) having knowledge of Engstrom's fraud and (2) orchestrating a scheme with Campion to sell worthless invoices to Millennium.

32. Before Millennium's deal with LSQ closed, Campion expressed concern that LSQ would alert Millennium to her Ponzi-like invoice scheme. For example, in a January 21, 2020, email to Bailey's Subject Account 1, Campion wrote:

> *I sent you an update yesterday on progress for repurchase of accounts. The partner I am working with diligently to get this all completed stated if needed they would confirm this is being worked on and doing due diligence on this end to get this completed this week they would reach out to you sine they would be the partner that would be paying off balance due and repurchase of accounts.*
>
> *I have a deep concern if they would reach out any statements would be made and was to me on the phone that would hurt my progress with them on getting LSQ paid back and purchasing of the invoices and get this taken care of and LSQ paid back. I can have them confirm to reach out that I am working on this to get completed but again have a concern on any statements that may be made that will put this all backwards on the progress we are making to get this completed. They are aware of many of the events and was honest to them about that end of it but, again, I have a concern on any statements that would be made that would hurt/put everything backwards on getting LSQ paid back in full through this due diligence process.*
>
> *If you could let me know on this and if you would like confirmation from the financing source that this is actually being taken care, please let me know. I will monitor my email regularly since in meetings a lot this week myself with client at their site and taking care of meetings with financing partner, etc., to get this also taken care of for payoff.*

33. Bailey, using Subject Account 1, replying to Campion's email, quickly dispelled her (Campion's) concerns:

> *Thanks, Cherie. We appreciate the update. We can provide a payoff letter which provides its own terms but we do not otherwise engage with third parties with regards to our clients.*

34. On January 28, 2020, Millennium, believing Engstrom's invoices to be legitimate, countersigned a payoff letter and wired approximately $10.3 million to LSQ. Millennium, witness interviews indicate, quickly discovered Engstrom's scheme after receiving the first purported payment from NextEra. The payment, records indicate, was in fact received from Campion's NextEra ES Account 7135. Millennium quickly confronted Campion in-person, who confessed to her long running Ponzi-like scheme. Campion told Millennium officials she believed LSQ knowingly sold worthless invoices to Millennium, pointing to telephone conversations she had with Bailey and other LSQ officials, including Lee and Ambrico.

35. Campion's belief that LSQ knowingly sold worthless invoices to Millennium was also discussed in her attorney's letter. Campion, the letter asserts, advised, "Every time LSQ asked questions, they never look into it until 2019 when they had a big audit coming up themselves and probably saw they needed concrete answers to their audit regarding Engstrom. Throughout all the years, I would say credit card payments or stupid excuses and they let it continue."

36. Records from Subject Accounts 1 & 2 will assist the investigation by revealing the existence of any communications pertaining to potentially corrupt dealings between Bailey, Lee, and other LSQ employees and officers, efforts to conceal

the discovery of Engstrom's fraud, possible perjurious statements made during subsequent legal proceedings, the identity of other relevant individuals involved in or knowledgeable about the Subject Offenses, if and when pertinent communications were exchanged, and communications devices possibly involved in violations of the Subject Offenses.

Microsoft Records

37. Records subpoenaed from Microsoft show that a business account was created under the lsq.com domain on January 29, 2017. The registered address for this account is 315 E Robinson St Suite 200, Orlando, FL. According to Florida's Division of Corporations, this is the same address as the principal and mailing address for LSQ Funding Group, L.C.

38. Microsoft records show the lsq.com domain account has had an active Exchange Online (Plan 1) subscription since June 26, 2019. This service is due to expire on June 26, 2023. Based on a search of Microsoft.com, Exchange Online (Plan 1) is an email hosting service for businesses that provides a 50 GB mailbox and messages up to 150 MB at a rate of $4 per user per month. It also automatically moves old messages to an In-Place Archive, among other services.

39. Microsoft records show the lsq.com domain account had an Office 365 E3 subscription from October 4, 2018 to November 30, 2019. Based on a search of Microsoft.com, Office 365 E3 is a cloud-based suite of apps and services including among others, Exchange Online and Microsoft OneDrive, at a rate of $36 per user per month.

40. Microsoft records show Subject Accounts 1 & 2 are user accounts under the lsq.com domain account. These records show user profiles were created for Carrie Bailey and Richard Lee on June 20, 2019. Bailey's user profile lists her mail as Subject Account 1 and Lee's user profile lists his mail as Subject Account 2. Furthermore, the records show the Subject Account 1 mailbox was create on August 7, 2019 and the Subject Account 2 mailbox was created on August 14, 2019.

BACKGROUND CONCERNING EMAIL

41. In my training and experience, I have learned that Microsoft provides a variety of online services, including electronic mail ("email") access, to other companies. Microsoft allows companies to obtain email accounts and tailor the domain names to their businesses, like the email accounts listed in Attachment A using "lsq.com". Subscribers obtain an account by registering with Microsoft. During the registration process, Microsoft asks subscribers to provide basic personal information. Therefore, the computers of Microsoft are likely to contain stored electronic communications (including retrieved and unretrieved email for Microsoft subscribers) and information concerning subscribers and their use of Microsoft services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

42. In my training and experience, I have learned that historical emails associated with a user's mailbox can be migrated to Microsoft's servers when the

user's enterprise subscribes to Microsoft Exchange services and migrates the user's mailboxes to Microsoft's servers. Therefore, emails preceding the date on which an enterprise user's mailbox was created on the Microsoft Exchange are likely stored on Microsoft's servers.

43. A Microsoft subscriber can also store other data with the provider files, in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Microsoft. In my training and experience, evidence of who was using an email account may be found in such data, to include address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

44. In my training and experience, I have learned that in general a sent/received email is stored in the subscriber's "mailbox" on the email service provider's server until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on the email service provider's server indefinitely. Even if the subscriber deletes the email, it may continue to be available on the service provider's server for a certain period of time.

45. In my training and experience, I have learned that email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including

any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

46. In my training and experience, I have learned that email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

47. In my training and experience, I have learned that in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such

communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

48. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline

information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

49. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Microsoft, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Grand Jury Matter Number 2021R00461

PROPERTY TO BE SEARCHED

This warrant applies to information associated with the following accounts that are stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, a company headquartered at One Microsoft Way, Redmond, WA 98052 (Subject Accounts 1 and 2):

1. cbailey@lsq.com
2. rlee@lsq.com

ATTACHMENT B

Grand Jury Matter Number 2021R00461

PARTICULAR THINGS TO BE SEIZED

I. Information to be disclosed by Microsoft Corporation (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to the request made under 18 U.S.C. § 2703(f) on January 4, 2023, the Provider is required to disclose the following information to the government for the accounts or identifiers listed in Attachment A:

a. The contents of all emails associated with the accounts from January 1, 2019 until the date of this warrant, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the

account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and

f. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within 21 days of the issuance of the warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18, United States Code, Sections 371 and 1343 involving Cherie Campion, Engstrom Inc., LSQ Funding Group, L.C., Carrie Bailey, and Richard Lee, those violations occurring after January 1, 2019, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Evidence of fraud, conspiracy, and related activity in connection with the purchase, sale, and payoff of invoices;

b. Evidence indicating knowledge and concealment of false invoices;

c. Evidence of financial transactions related to the purchase, sale, and payoff of invoices;

d. Evidence of audits, examinations, and background checks;

e. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

f. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

g. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

h. The identity of person(s) who communicated with the account about matters relating to the criminal violations described above, including records that help reveal their whereabouts.